PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(54) Title: LINK AND RADIO CELL ADAPTATION IN TDMA/TDD SYSTEMS

(57) Abstract

A TDMA/TDD link adaptation method determines radio link quality at a base station. The radio link quality is used to update and broadcast a physical layer parameter indicator (10–16) from the base station on a broadcast control channel having a common physical layer parameter indicator for all uplink and downlink channels.

LINK AND RADIO CELL ADAPTATION IN TDMA/TDD SYSTEMS

TECHNICAL FIELD

5   The present invention relates generally to TDMA/TDD (Time Division Multiple Access / Time Division Duplex) radio communication systems, and especially to adaptation of the systems to prevailing radio conditions.

BACKGROUND

10

ETSI BRAN (Broadband Radio Access Network) is developing a short-range high data rate system, HIPERLAN Type 2 (also called H/2), mainly for indoor operation. Some outdoor scenarios are also considered (campus areas, downtown city areas). The target areas are offices, conference halls,

15   exhibition fairs, airports and home environments. The spectrum is unlicensed and thus several "operators" may use the same spectrum. The interference environment may change during operation due to for example new operators in the vicinity of the own network and it is then very difficult to predict what type of interference the system shall be able to handle. The

20   large difference in radio propagation, i.e. LOS (Line Of Sight) and NLOS (No Line Of Sight), and interference environments in which the system be must be able to operate, puts strong requirements on the system that it is able to adapt to its current situation. In this type of systems, one radio cell might be exposed to larger interference than other radio cells. Just an adaptation per

25   radio cell to handle this situation is referred to as "radio cell adaptation". Furthermore, the mobile terminals (MTs) associated with a certain base station (BS) may have different reception qualities in their uplink and downlink respectively. Hence, in this case each MT might want to use different transmission parameters, e.g. code rate (protection level) and

30   modulation alphabet, to be able to adjust its reception quality in the uplink and downlink. This adaptation could be performed per MT or per its individual connections. In the latter case differing traffic and QoS (Quality of

Service) parameters have to be considered. For example, one MT could have a connection carrying video using a powerful FEC (Forward Error Correction) code, whereas a connection for file transfer uses a less strong FEC but with ARQ (Automatic ReQuest for retransmission) capabilities.

5

Typical reception quality measures are:

    retransmission rate (PER, Packet Error Rate),
    delay spread (time dispersion),
10 received signal strength (RSSI),
    Signal-to-Interference Ratio (SIR)
    Bit Error Rate (BER)

Combinations of these performance measures and others are also possible.
15

Usually link adaptation is divided into two groups: net rate adaptation and gross rate adaptation.

Net rate adaptation means that the incoming data rate is adjusted to fit into
20 the assigned capacity so that the system can handle a certain link quality, i.e. the user has a fixed assigned capacity over the air, and if the radio quality is poor the incoming data rate is reduced and a more robust transmission mode is used. In case of a good connection a higher incoming data rate can be used.

25

In gross rate adaptation the incoming data rate is "fixed", i.e. the radio system does not change its incoming traffic due to the radio conditions. Instead the radio system tries to sustain the incoming data rate and to counter the variations in link quality by assigning correspondingly varying
30 capacity over the air interface. Thus, two MT with the same incoming data rate could have been assigned different capacity over the air interface based on their individual connection reception qualities. An extra function might be

needed in this case to guarantee fair utilisation of the total available capacity.

Combination of net and gross rate adaptation is of course also possible.

The present situation with regard to adaptation to varying radio conditions in different radio communication standards may be summarised as follows:

HIPERLAN/2: No proposal exists on a protocol that handles the ability to make radio cell adaptation and/or link (per MT or per connection) adaptations. Still, the proposals on the physical layer allow different code rates and modulation alphabets (MPSK and MQAM signal constellations).

GPRS: The system applies net rate link adaptation (selects channel coding) per mobile terminal, see [1]. For downlink traffic the MT request channel coding via ARQ-ACK/NACK messages through the uplink. The BS is using stolen bits (embedded in the burst structure of GSM) to set the channel code for the downlink. Hence, the MT first decodes these bits to obtain information on which channel decoding it shall use for the rest of the burst. In case unacknowledged mode is applied, the MT sends measurements reports to the BS including an estimation of the BER. This information can then be used by the BS to select channel coding for the downlink bursts.

For the uplink traffic the BS commands the MT to use a certain channel coding. This information is transferred to the MT piggybacked on downlink dedicated control channels, e.g. piggybacked on ARQ-ACK/NACK messages.

A drawback is that in GRPS it is not possible to change channel coding during retransmission phase.

EDGE, EGPRS: These two systems apply net rate link adaptation (select channel coding and modulation alphabet) per mobile terminal. No protocol exists yet. However, the structure and protocol is based on the GPRS

structure and a similar protocol will be utilised. Extensive simulation studies have been performed on the system throughput and can be found in [2].

The problem with changing channel coding during retransmissions is solved by doing re-segmentation. However, the frame structure used in these systems is not suited for a TDD system.

DVB, DAB: Digital Video/Audio Broadcasting uses different code rates and modulation alphabets to be able to extend their coverage regions and to enable the possibility for an broadcaster to select suitable parameters so that both data and the ordinary program can be sent on the allocated bandwidth, see [3]. In the pure broadcast scenario no uplink signalling exists. Recently, an ACTS program called MEMO has been developed for individual services; the ordinary GSM network is used for the uplink signalling. In this case downlink link adaptation is possible. Still no protocol that enables this signalling exists.

IEEE 802.11: A new physical layer standard is now developed for 5 GHz operation, see [4]. The standard is not fixed yet and the system will apply some sort of link adaptation. The proposed solution is assuming that the physical layer is totally independent from the IEEE 802.11 MAC layer. To enable this a convergence layer, called PHY PLCP (Physical Layer Convergence Protocol), is put in between, where primitives are used through SAPs (Service Access Point) to instruct the physical layer to react.

The selected link parameters are performed by the sending unit, i.e. in the downlink the BS selects the parameters and in the uplink the MT selects the parameters. Both BS and MT are making measurements before selecting PHY (PHYsical layer) parameters, e.g. RSSI measurements.

The access scheme is based on CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). This implies that one MAC frame (in IEEE 802.11 this is equal to a MPDU (MAC Protocol Data Unit)) is transmitted between

two peer entities only, i.e. the MAC frame is only between a BS (centrally controlled system) and one MT, or the MAC frame is only between two MTs (Ad-hoc system). The duration of the MAC frame depends on the selected PHY parameter In case of a more robust PHY mode, the length of the PHY frame becomes longer due to higher FEC protection.

This is a gross rate adaptation approach which is not able to consider QoS and fairness between users, i.e. since the transmitting unit is selecting the PHY parameters (used capacity), a user may select a parameter corresponding to a robust PHY mode resulting in larger capacity utilisation even though it is not necessary.

In the current version of the IEEE 802.11 proposal for 5 GHz, measurements needed for the selection of PHY parameters has to be performed by both the BS and the MT.

SUMMARY

An object of the present invention is to provide a spectrum efficient radio link adaptation method and frame structure for a TDMA/TDD radio communication system..

This object is achieved in accordance with the attached claims.

Briefly, the present invention uses the BCCH (Broadcast Control CHannel) to adapt the radio cell to prevailing radio conditions. This provides a very efficient method, since a common physical layer parameter indicator may be used for all radio links. An efficient and more flexible embodiment uses a common physical layer parameter indicator to adapt the uplinks of the radio cell, while the downlinks are individually adapted using physical layer parameter indicators in the ACH (Announcement & assignment CHannel). It

is also possible to let the BCCH indicate the physical layer parameters to be used for decoding of the ACH.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention, together with further objects and advantages thereof, may best be understood by making reference to the following description taken together with the accompanying drawings, in which:

Fig. 1 is a diagram illustrating a basic frame structure of a TDMA/TDD radio communication system;

Fig. 2 is a diagram illustrating an exemplary embodiment of a frame structure in accordance with the present invention suitable for a TDMA/TDD radio communication system; and

Fig. 3 is a diagram illustrating another exemplary embodiment of a frame structure in accordance with the present invention suitable for a TDMA/TDD radio communication system.

DETAILED DESCRIPTION

The system in accordance with the present invention uses a TDMA/TDD (Time Division Multiple Access/Time Division Duplex) MAC (Media Access Control) frame structure (e.g. H/2 and IEEE 802.11). An example of such a frame structure is depicted in fig. 1. A centrally controlled MAC scheme is assumed, i.e. the BS assigns capacity to the MTs. The assignments could be different between two MAC frames, i.e. one user might be assigned capacity in one MAC frame and in the next MAC frame this user will not be assigned any capacity. In case of ad-hoc operation, one MT could act as the central controller. In fig. 1 assigned capacity for one connection (downlink + uplink) has been indicated, while the dots represent assigned capacity for other connections.

The MAC frame starts with a Broadcast Control CHannel (BCCH) which contains information that is transmitted over the entire area that a BS covers (radio cell). The assignment of different MTs capacity is transmitted in the ACH (Announcement & assignment CHannel, sometimes referred to as

5   resource grant channel or FCH (Frame Control cHannel)). The whole ACH is not necessarily transmitted over the whole radio cell. In case multi beam antennas are applied, the information that is only concerned to a certain beam is then only transmitted over its corresponding coverage area. Pointers may be applied in the ACH so that a MT that is assigned capacity knows

10   exactly when in the frame it is expected to receive and send data, i.e. in the "Assigned Capacity" regions. Random Access CHannels (RACH) might be located at the end of the frame. A MT may request for capacity in its assigned uplink capacity region or via one random access channel.

15   The exemplary embodiments of frame structures in accordance with the present invention described below are applicable for both gross and net rate link/radio cell adaptation.

Fig. 2 is a diagram illustrating an exemplary embodiment of a frame

20   structure in accordance with the present invention suitable for a TDMA/TDD radio communication system with centrally controlled assignment of capacity. In this embodiment radio cell adaptation parameters are only transmitted in the BCCH (or some other permanent or temporary "control channel" for broadcasting messages). This embodiment may assume that the

25   BS has all information necessary to make a decision on a single PHY parameter setting (e.g. code rate, modulation alphabet, time slots/frame) without any interaction (no explicit uplink signalling) with the MTs). Statistics of the PER, delay spread, received signal strength, SIR and BER could for example be used in the selection procedure. The measurements

30   could be performed on the traffic and control data PDUs (Protocol Data Units) that are received at the BS. The single PHY parameter setting (which is dynamically varying) could be used for some or all connections, as indicated by the dashed arrows 10, 12, 14 and 16 in fig. 2.

One nice feature of this embodiment is that all PDUs of the same type will have the same size and the assignment of capacity resources becomes easier.

Since a common indicator is used for all links, it is appreciated that the embodiment in fig. 1 implements radio cell adaptation.

Radio cell adaptation could also be performed on uplink only or downlink only. Furthermore, the broadcast message including the common PHY parameter indicator may also be broadcast in other "channels" than the BCCH, for example a dedicated PHY parameter channel.

Fig. 3 is a diagram illustrating another exemplary embodiment of a frame structure in accordance with the present invention suitable for a TDMA/TDD radio communication system. In this embodiment a single PHY mode is used in the uplink for all MTs, as indicated by dashed arrows 10, 12. This is an efficient signalling mechanism in case all MT will have similar reception quality in the uplink. This could for example be accomplished if power control is applied in the uplink, i.e. the BS controls (decides) the MTs power level. However, in this embodiment the downlink is individually assigned via the ACH, as indicated by dashed arrows 18, 20 in fig. 3.

The embodiment of fig. 3 implements a combination of radio cell and individual link adaptation, since all uplinks are adapted in the same way as in the embodiment of fig. 1, while downlinks are individually adapted.

A combination of the embodiments of fig. 2 and 3 is also possible. In such a combination the BCCH (or some other permanent or temporary "control channel" for broadcasting messages) is used to broadcast an indicator of the physical layer parameters that should be used to decode the ACH. The physical layer parameters may be individual or common for several channels,

In some cases it is not necessary for the MTs to update the BS so frequently. This could be in situations when the radio channel and the interference environment are rather static and do not change. To use the ARQ PDU for this signalling will then create unnecessary overhead. To reduce the amount of signalling, a special signalling message (control channel), in which the information is transferred, could be used. This is a special control channel that is separated from other channels. An initial negotiation could take place between the MT and the BS on how often these messages should be transmitted. The BS could then, for example, assign uplink capacity to the MT on a regular basis. Such an embodiment creates a flexible solution. How the information is transmitted to the BS could also be negotiated, e.g. the approach to use the ARQ messages could of course be one way. Another approach is that all updates of the PHY mode are sent through the RACH. An alternative is to "piggyback" the information on one or several other messages, since this type of information may be represented by very few bits.

It will be understood by those skilled in the art that various modifications and changes may be made to the present invention without departure from the scope thereof, which is defined by the appended claims.

REFERENCES

[1]   Digital cellular telecommunications system (Phase 2+); General Packet Radio Services (GPRS); Mobile Station (MS) – Base Station System (BSS) interface; Radio Link Control/ Medium Access Control (RLC/MAC) protocol (GSM 04.60 proposed version 1.1.0)

[2]   Johansson C., de Verdier L., Khan F., "Performance of Different Scheduling Strategies in a Packet Radio System", VTC'98, 1998

[3]   Lindberg, A., "Aspects on individual services in a dense cellular broadcasting network", MSc Thesis.

[4]   Richard, Hitoshi, Masahiro, Doc: IEEE P802.11-98/74-r4, July 1998

CLAIMS

1.   A TDMA/TDD media access control frame structure, **characterized** by a broadcast message having a common dynamically updated physical layer parameter indicator for a plurality of channels.

2.   The control frame structure of claim 1, **characterized** by a broadcast message having a common dynamically updated physical layer parameter indicator for a plurality of uplink channels.

3.   The control frame structure of claim 1, **characterized** by a broadcast message having a common dynamically updated physical layer parameter indicator for a plurality of downlink channels.

4.   The control frame structure of claim 1, **characterized** by a broadcast message having a common dynamically updated physical layer parameter indicator for a plurality of uplink channels and a plurality of downlink channels.

5.   The control frame structure of any of the preceding claims, **characterized** by said broadcast message indicating the proper physical layer parameter that is to be used by a receiver to decode an announcement and assignment channel.

6.   The control frame structure of claim 2, **characterized** by an announcement and assignment channel having individual dynamically updated physical layer parameter indicators for downlink channels.

7.   The control frame structure of claim 6, **characterized** by said broadcast message indicating the proper physical layer parameter that is to be used by a receiver to decode an announcement and assignment channel.

8. The control frame structure of any of the preceding claims, **characterized** by said broadcast message belonging to a broadcast control channel.

9. The control frame structure of any of the preceding claims, **characterized** by a separate control channel for occasional requests of physical layer parameter updates from mobile terminals.

10. A TDMA/TDD link adaptation method, **characterized** by
    determining radio link quality at a central controller; and
    updating and broadcasting a message including a common physical layer parameter indicator for a plurality of channels from said central controller.

11. The method of claim 10, **characterized** by said message including a common physical layer parameter indicator for a plurality of uplink channels.

12. The method of claim 10, **characterized** by said message including a common physical layer parameter indicator for a plurality of downlink channels.

13. The method of claim 10, **characterized** by said message including a common physical layer parameter indicator for a plurality of uplink channels and a plurality of downlink channels.

14. The method of any of the preceding claims 10-13, **characterized** by said message indicating the proper physical layer parameter that is to be used by a receiver to decode an announcement and assignment channel.

15. The method of claim 11, **characterized** by an announcement and assignment channel for individually and dynamically updating physical layer parameter indicators for downlink channels.

16. The method of claim 15, **characterized** by said message indicating the proper physical layer parameter that is to be used by a receiver to decode an announcement and assignment channel.

5   17. The method of any of the preceding claims 10-16, **characterized** by said message belonging to a broadcast control channel.

18. The method of any of the preceding claims 10-17, **characterized** by a separate control channel for occasional requests of physical layer parameter

10   updates from mobile terminals.

19. The method of any of claims 10-18, **characterized** by said central controller being a base station.

15   ---

Fig. 1

Fig. 2

Fig. 3

PCT

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(54) Title: LINK AND RADIO CELL ADAPTATION IN TDMA/TDD SYSTEMS

(57) Abstract

A TDMA/TDD link adaptation method determines radio link quality at a base station. The radio link quality is used to update and broadcast a physical layer parameter indicator (10–16) from the base station on a broadcast control channel having a common physical layer parameter indicator for all uplink and downlink channels.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 99/01774

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04Q 7/38, H04B 7/26
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04B, H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 9832265 A1 (NOKIA TELECOMMUNICATIONS OY), 23 July 1998 (23.07.98), page 5, line 4 - line 30; page 5, line 35 - page 6, line 7; page 6, line 13 - line 37, claim 7	1-4,6,8, 10-13,15, 17-19
A		5,7,14,16
	--	
A	WO 9826523 A2 (ERICSSON INC.), 18 June 1998 (18.06.98), page 3, line 32 - page 4, line 2; page 13, line 31 - line 33; page 14, line 18 - page 15, line 7, page 15, line 33 - page 16, line 15	1-19
	--	
A	US 5329574 A (NIELSON ET AL), 12 July 1994 (12.07.94), column 3, line 26 - line 53	10
	--	

[X]	Further documents are listed in the continuation of Box C.	[X] See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 March 2000	0 4 -04- 2000

Name and mailing address of the ISA/	Authorized officer
Swedish Patent Office	
Box 5055, S-102 42 STOCKHOLM	Peter Göransson / JA A
Facsimile No. + 46 8 666 02 86	Telephone No. + 46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 99/01774

C (Continuation).   DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,X	WO 9907168 A1 (BELLSOUTH CORPORATION), 11 February 1999 (11.02.99), claims 1,2,4, abstract	1,10

INTERNATIONAL SEARCH REPORT

Information on patent family members

02/12/99

Patent document cited in search report			Publication date	Patent family member(s)			Publication date
WO	9832265	A1	23/07/98	AU	5665398	A	07/08/98
				FI	3052	U	12/09/97
				FI	970237	A,V	21/07/98
				ZA	9800162	A	09/07/98
WO	9826523	A2	18/06/98	AU	5607398	A	03/07/98
				US	5896376	A	20/04/99
US	5329574	A	12/07/94	NONE			
WO	9907168	A1	11/02/99	AU	8585598	A	22/02/99

Form PCT/ISA/210 (patent family annex) (July 1992)

(54) Method for securely communicating remote control commands in a computer network

(57) A method for providing secure remote control commands in a distributing computer environment. In the preferred embodiment of the invention, a network administrator or network management software creates a shutdown record, including an index or time stamp, for powering down a specified network computer(s). Prior to broadcast over the network, a secure one-way hash function is performed on the shutdown record. The result of the one-way hash function is encrypted using the network administrator's private key, thereby generating a digital signature that can be verified by specially configured network nodes. The digital signature is appended to the original shutdown record prior to broadcast to the network. Upon receiving the broadcast message, the targeted network computer(s) validates the broadcast message by verifying the digital signature of the packet or frame. The validation process is performed by decrypting the hash value representation of the shutdown record using the network administrator's public key. A one-way hash function is also performed on the original shutdown record portion of the received message. If the two values match, the broadcast message is determined to be authentic and the shutdown control code is executed. The invention insures that the shutdown command was neither modified in transit nor originated from an unauthorized source.
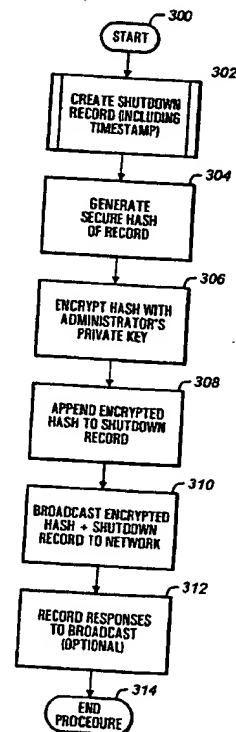
FIG. 3

Description

[0001] The invention relates to security in a computer network, and more particularly to a secure method for communicating remote control commands in a distributed computing environment.

[0002] A majority of today's businesses utilize some form of computer network. As servers and clients are deployed into more mission critical environments and used in more remote areas, the amount of human resources required to manage these computer networks is growing. Computer networks are often maintained by either a network administrator or an Information Systems (IS) department. Network administrators are often tasked with performing such duties as data backups or software updates on network computers at times when network users will not be negatively impacted (e.g., at night). These tasks are simplified somewhat by relatively new network management hardware and software that allows remote access to network computers. To remotely access network computers, however, requires that network users leave machines running or disable energy saving features. This requirement can conflict with efforts to reduce computer power consumption.

[0003] In particular, the Environmental Protection Agency (EPA) has attempted, through the Energy Star Program, to reduce computer power consumption via the creation of so-called "green" computers. The term "green computer" typically refers to a computer that enters low-power mode following a specified period of inactivity. The proliferation of green computers in networks, while laudable, can interfere with a network administrator's duties. For example, if a network computer is in sleep mode (or other low power state) it often cannot be addressed from the network.

[0004] Attempts have been made to alleviate this problem. For example, Magic Packet™ technology, a proposed industry standard jointly developed by Advanced Micro Devices and Hewlett-Packard Corporation, provides a mechanism whereby a network administrator or network management software can "wake up" or power down a network computer by sending it a special Ethernet frame. Briefly, the Ethernet frame includes a specific data pattern that can be detected by a specially configured network interface controller incorporated in a network computer. The network interface controller is capable of communicating with the network computer's power management hardware or software to power up or power down the network computer in response to a control code portion of the special Ethernet frame.

[0005] In addition to networking hardware and software, today's businesses also invest large amounts of money developing information contained in data files such as text documents and spreadsheets. Protecting such investments can be critical to the success and reputation of a business. Public accounts of the exploits of computer "hackers" -- as malicious code-breakers or eavesdroppers are sometimes called -- have therefore focussed and magnified corporate desires for secure communications and better methods of protecting data. The scope of the problem is undoubtedly even more serious than reported, given the reluctance of many businesses to publicize security breaches. As a result, computer manufacturers and network software developers are striving to incorporate security and integrity features into their products to restrict access to data contained on network hard drives, as well as information contained in other critical network components.

[0006] One known approach to security involves encryption or cryptography. Cryptography is typically used to protect both data and communications. Generally, an original message or data item is referred to as "plain text", while "encryption" denotes the process of disguising or altering a message in such a way that its substance is not readily discernable. An encrypted message is sometimes called "ciphertext". Ciphertext is returned to plain text by an inverse operation referred to as "decryption". Encryption is typically accomplished through the use of a cryptographic algorithm, which is essentially a mathematical function. The most common cryptographic algorithms are key-based, where special knowledge of variable information called a "key" is required to decrypt ciphertext. There are many types of key-based cryptographic algorithms, providing varying levels of security.

[0007] The two most prevalent cryptographic algorithms are generally referred to as "symmetric" (also called secret key or single key algorithms) and "public key" (also called asymmetric algorithms). The security in these algorithms is entered around the keys -- not the details of the algorithm itself. This makes it possible to publish the algorithm for public scrutiny and then mass produce it for incorporation into security products.

[0008] In symmetric algorithms, the encryption key and the decryption key are the same. This single key encryption arrangement is not without drawbacks. The sender and recipient of a message must somehow exchange information regarding the secret key. Each side must trust the other not to disclose the key. Further, the sender must generally communicate the key via another media (similar to a bank sending the personal identification number for an AIM card through the mail). This arrangement can be impractical, for example, when the parties interact electronically for the first time over a network. The number of keys also increases rapidly as the number of users increases.

[0009] With public key algorithms, by comparison, the key used for encryption is different from the key used for decryption. It is generally very difficult to calculate the decryption key from an encryption key. In typical operation, the "public key" used for encryption is made public via a readily accessible directory, while the corresponding "private key" used for decryption is known only to the recipient of the ciphertext. In an exemplary public key transaction, a sender retrieves the recipient's

public key and uses it to encrypt the message prior to sending it. The recipient then decrypts the message with the corresponding private key. It is also possible to encrypt a message using a private key and decrypt it using a public key. This is sometimes used in digital signatures to authenticate the source of a message.

[0010] The number of cryptographic algorithms is constantly growing. The two most popular are DES (Data Encryption Standard) and RSA (named after its inventors -- Rivest, Shamir, and Adleman). DES is a symmetric algorithm with a fixed key length. RSA is a public key algorithm that can be used for both encryption and digital signatures. DSA (Digital Signature Algorithm) is another popular public key algorithm that is only used for digital signatures. With any of these algorithms, the relative difficulty of breaking an encrypted message by guessing a key with a brute force attack is proportional to the length of the key. For example, if the key is 40 bits long (5 characters), the total number of possible keys (2^{40}) is about 110 billion. Given the computational power of modern computers, this value is often considered inadequate. By comparison, a key length of 56 bits (7 characters) provides 65,636 times as many possible values as the 40 bit key.

[0011] One problem with key-based algorithms is speed. Public key algorithms, in particular, are typically on the order of 1,000 times slower than symmetric algorithms. Even symmetric algorithms can be slow when compared with so-called "one-way functions" or "one-way hash functions".

[0012] Briefly, an ideal one-way hash function, denoted H(M), operates on an arbitrary-length block of text or message M. The one-way hash function returns a fixed-length hash value, h, such that h = H(M), where h is of length m. One-way hash functions have special characteristics that make them one-way. Given M, for example, it is easy to compute h. Given h, it is impossible to reverse the hashing process and compute M such that H(M) = h. Further, it is impossible to find another message, M', such that H(M) = H(M'). In essence, the one-way hash function provides a "fingerprint" of M that is unique, and is therefore useful for purposes of authenticating the source of a message.

[0013] Briefly, a computer system according to the present invention provides a secure method for communicating remote control commands in a distributed computing environment. A potential problem with providing remote control capabilities in a computer network is that unauthorized users may broadcast shutdown or wake up commands to network nodes in an undesirable manner. A system according to the present invention addresses this concern.

[0014] According to the invention, a network administrator or network management software creates a shutdown (or other control command) record including an index or time stamp with the date and time on which the shutdown record was created. A secure one-way hash function is then performed on the shutdown record. The result of the one-way hash function is encrypted using the network administrator's private key, thereby generating a digital signature of the shutdown record that can be verified by network nodes using the network administrator's public key. The digital signature is appended to the original shutdown record prior to broadcast to the network.

[0015] Following detection of a broadcast message addressed to it, a network computer according to the invention is able to validate the broadcast message by verifying the digital signature of the packet or frame. In the disclosed embodiment, the validation process is performed by decrypting the hash value representation of the shutdown record using the network administrator's public key. A one-way hash function is also performed on the original shutdown record portion of the received message. If the two hash values match, the broadcast message is determined to be authentic and the shutdown control code is executed.

[0016] The present invention thereby protects and authenticates remote control commands transmitted via corporate networks, intranets and LANs. Unauthorized users and malicious software are prevented from turning off (or waking up) network computers or performing other unauthorized functions such as malicious alteration of ROM code. For machines in which it is desirable to disable remote control functionality, it is also contemplated that the public key of the network administrator can be invalidated such that the specified machine is incapable of detecting a valid broadcast message.

[0017] A better understanding of the present invention can be obtained when the following detailed description of the preferred embodiment is considered in conjunction with the following drawings, in which:

Figure 1 is a schematic block diagram of a network computer system incorporating networking capabilities in accordance with the present invention;

Figure 2 is a schematic block diagram of an exemplary local area network capable of secure remote control communications according to the present invention;

Figure 3 is a flowchart diagram illustrating generation of a secure network broadcast message in accordance with the present invention; and

Figure 4 is a flowchart diagram illustrating the receipt and validation of a secure network broadcast message in accordance with the present invention.

[0018] The following patents and applications are referenced below:

Commonly owned U.S. Patent Application Serial No. 08/766,721, entitled "A METHOD AND APPARATUS FOR ALLOWING ACCESS TO SECURED COMPUTER RESOURCES BY UTILIZING A PASSWORD AND EXTERNAL ENCRYPTION ALGORITHM", filed on December 13, 1996;

Commonly owned EP-A-0 851 335, entitled "SE-
CURE TWO-PIECE USER AUTHENTICATION IN
A COMPUTER NETWORK"; and

Commonly owned U.S. Patent Application Serial
No. 08/777,615, entitled "METHOD FOR SECURE-
LY CREATING, STORING AND USING ENCRYP-
TION KEYS IN A COMPUTER SYSTEM", filed on
December 31, 1996.

[0019]   Referring first to Figure 1, a network computer
system incorporating networking capabilities in accord-
ance with the present invention is shown. In the pre-
ferred embodiment, the network computer S incorpo-
rates two primary buses: a Peripheral Component Inter-
connect (PCI) bus P which includes an address/data
portion and a control signal portion; and an Industry
Standard Architecture (ISA) bus I which includes an ad-
dress portion, a data portion, and a control signal por-
tion. The PCI and ISA buses P and I form the architec-
tural backbone of the network computer S.
[0020]   A CPU/memory subsystem 100 is connected
to the PCI bus P. The processor 102 is preferably the
Pentium® or Pentium II® processor from Intel Corpora-
tion, or any number of similar or next-generation proc-
essors. The processor 102 drives data, address, and
control portions 116, 106, and 108 of a host bus HB. A
level 2 (L2) or external cache memory 104 is connected
to the host bus HB to provide additional caching capa-
bilities that improve the overall performance of the net-
work computer S. The L2 cache 104 may be permanent-
ly installed or may be removable if desired. Alternatively,
the L2 cache 104 may be embodied within the 102. A
cache and memory controller 110 and a PCI-ISA bridge
chip 130 are connected to the control and address por-
tions 108 and 106 of the host bus HB. The cache and
memory controller chip 110 is configured to control a se-
ries of data buffers 112. The data buffers 112 are pref-
erably the 82433LX from Intel, and are coupled to and
drive the host data bus 116 and a MD or memory data
bus 118 that is connected to a memory array 114. A
memory address and memory control signal bus is pro-
vided from the cache and memory controller 110.
[0021]   The data buffers 112, cache and memory con-
troller 110, and PCI-ISA bridge 130 are all connected to
the PCI bus P. The PCI-ISA bridge 130 is used to convert
signals between the PCI bus P and the ISA bus I. The
PCI-ISA bridge 130 includes: the necessary address
and data buffers, arbitration and bus master control logic
for the PCI bus P, ISA arbitration circuitry, an ISA bus
controller as conventionally used in ISA systems, an IDE
(intelligent drive electronics) interface, and a DMA con-
troller. A hard disk drive 140 is connected to the IDE
interface of the PCI-ISA bridge 130. Tape drives, CD-
ROM devices or other peripheral storage devices (not
shown) can be similarly connected.
[0022]   In the disclosed embodiment, the PCI-ISA
bridge 130 also includes miscellaneous system logic.
This miscellaneous system logic contains counters and

activity timers as conventionally present in personal
computer systems, an interrupt controller for both the
PCI and ISA buses P and I, and power management
logic. Additionally, the miscellaneous system logic pref-
erably includes circuitry for a security management sys-
tem used for password verification and to allow access
to protected resources. For example, the PCI-ISA
bridge 130 of the disclosed embodiment includes vari-
ous address decode logic and security logic to control
access to an internal or external CMOS/NVRAM mem-
ory (not shown) and stored password values. The
CMOS/NVRAM memory is coupled to the PCI-ISA
bridge 130 via a standard I²C bus (also not shown).
[0023]   The PCI-ISA bridge 130 also includes circuitry
to generate a firmware initiated SMI (System Manage-
ment Interrupt), as well as SMI and keyboard controller
interface circuitry. The miscellaneous system logic is
connected to the flash ROM 154 through write protec-
tion logic 164. Separate enable/interrupt signals are al-
so communicated from the PCI-ISA bridge 130 to the
hard drive 140. Preferably, the PCI-ISA bridge 130 is a
single integrated circuit, but other combinations are pos-
sible.
[0024]   A series of ISA slots 134 are connected to the
ISA bus I to receive ISA adapter cards. A series of PCI
slots 142 are similarly provided on the PCI bus P to re-
ceive PCI adapter cards.
[0025]   A video controller 165 is also connected to the
PCI bus P. Video memory 166 is used to store graphics
data and is connected to the video graphics controller
165 and a digital/analog converter (RAMDAC) 168. The
video graphics controller 165 controls the operation of
the video memory 166, allowing data to be written and
retrieved as required. A monitor connector 169 is con-
nected to the RAMDAC 168 for connecting a monitor
170.
[0026]   A combination I/O chip 136 is connected to the
ISA bus I. The combination I/O chip 136 preferably in-
cludes a real time clock, two UARTS, and a floppy disk
controller for controlling a floppy disk drive 138. Addi-
tionally, a control line is provided to the read and write
protection logic 164 to further control access to the flash
ROM 154. Serial port connectors 146 and parallel port
connector (not shown) are also connected to the com-
bination I/O chip 136.
[0027]   An 8042, or keyboard controller, is also includ-
ed in the combination I/O chip 136. The keyboard con-
troller is of conventional design and is connected in turn
to a keyboard connector 158 and a mouse or pointing
device connector 160. A keyboard 159 is connected to
the network computer S through the keyboard connec-
tor 158.
[0028]   A buffer 144 is connected to the ISA bus I to
provide an additional X-bus X for various additional
components of the network computer S. A flash ROM
154 receives its control, address and data signals from
the X-bus X. Preferably, the flash ROM 154 contains the
BIOS information for the computer system and can be

remotely reprogrammed to allow for revisions of the BI-OS.

[0029] In the disclosed embodiment, the network computer S contains circuitry for communicating with a removable cryptographic token 188. The token can take many forms, such as a Touch Memory™ device supplied by Dallas Semiconductor, Inc., a smart card, or an encryption card. The token 188 is easily decoupled from the network computer S and easily transportable by the token bearer. The token 188 preferably contains at least one of a variety of encryption algorithms (such as DES, Blowfish, elliptic curve-based algorithms, etc.). Although the base algorithm can be the same in each token 188, it is desirable that the encryption key be different in each token 188. Ideally, the token 188 is capable of communicating digitally with the network computer S during momentary contact with or proximity to the network computer S. The token 188 of the disclosed embodiment is capable of storing the encryption algorithm in a non-volatile manner and can be permanently write-protected to discourage tampering. Use of such tokens is further described in the previously incorporated patent application entitled "A METHOD AND APPARATUS FOR ALLOWING ACCESS TO SECURED COMPUTER RESOURCES BY UTILIZING A PASSWORD AND AN EXTERNAL ENCRYPTION ALGORITHM".

[0030] In the disclosed embodiment of the invention, the circuitry used for establishing a communication link between the token 188 and the network computer S consists of a probe 186 connected to a COM or serial port adapter 184. The port adapter 184 is connected to the RS232 connector 146. In operation, the token 188 is detachably received by the probe 186. The probe 186 includes circuitry for reading and writing memory in the token 188, and can be fully powered through the RS232 connector 146. In addition, the probe 186 includes presence detector circuitry for ascertaining the presence of a token 188.

[0031] A network interface controller (NIC) 122 incorporating remote control capabilities, such as those described more fully below, is also connected to the PCI bus P, allowing the network computer S to function as a "node" on a network. Preferably, the network interface controller 122 is a single integrated circuit that includes the capabilities necessary to act as a PCI bus-master and slave, as well as circuitry required to act as an Ethernet interface. Attachment Unit Interface (AUI) and 10 base-T connectors (not shown) are provided in the system S, and are connected to the NIC 122 via filter and transformer circuitry. This circuitry forms a network or Ethernet connection for connecting the network computer S to a distributed computer environment or local area network (LAN) as shown in Figure 2. The network interface controller 122 can be located on the motherboard and connected to a network via an RJ-45 connector (not shown). This configuration is becoming more popular as Ethernet gains widespread acceptance for desktop networking.

[0032] Most of today's personal computers also incorporate some form of advanced power management hardware/software 180 (such as Compaq Power Management Software) for controlling power distribution from a power supply 182. The power management hardware/software 180 typically allows the network computer S to be placed in any one of a number of different power down states, from merely reducing processor clock speed to powering down everything except the network interface controller 122. In a typical computer system S, the power management hardware/software 180 scans for any one of several events that serve to wake up the system. Such events may include keyboard 159 keystrokes or mouse movement. A Magic Packet™ indication signal can easily be included among the specified wake-up or power down events.

[0033] The network interface controller 122 is supplied with power by an auxiliary portion of power source 182 and is capable of communicating with a network (see Figure 2). Further, with the Magic Packet™ mode (discussed more fully below) enabled, the network interface controller 122 is capable of alerting the network computer's S power management hardware/software 180 following receipt of a valid Magic Packet™ frame. Conversely, the computer's power management hardware/software 180 is able to place the network interface controller 122 into Magic Packet™ mode prior to the computer system S entering a low power state. This can be accomplished, for example, by either setting a bit in an internal register or by driving a specified pin to a specified state. Once in Magic Packet™ mode, the network interface controller 122 no longer transmits frames, and scans all incoming frames addressed to it for a specific data sequence indicating that the frame is a Magic Packet™ frame. The Magic Packet™ frame must comply with the basic requirements of the chosen LAN technology, such as source address, destination address, and CRC.

[0034] The precise nature of the remote control networking mechanism is not considered critical to the invention and can take many forms, even within the confines of the Magic Packet™ standard. Most network interface controllers 122 already incorporate address matching circuitry to recognize regular frames address to the node. This circuitry can generally be adapted for use with the Magic Packet™ standard. Counter circuitry, in particular, may need to be added to the address matching circuitry.

[0035] It is noted that Figure 1 presents an exemplary embodiment of the network computer S and it is understood that numerous other effective embodiments capable of operation in accordance with the present invention could readily be developed as known to those skilled in the art.

[0036] Referring now to Fig. 2, an exemplary distributed access environment capable of secure remote control communications according to the present is shown. The disclosed network 200 includes a network administrator computer 202 and a plurality of network comput-

ers S, depicted as network computers 204, 206 and 208. A network interface controller 214 of the network administrator computer 202 communicates with a network interface controller 122 in each of the network computers S. Components of the network 200 are coupled via a network connection 208. Although Magic Packet™ or similar technology is not limited to anyone particular type of network connection 208, a 10BASE-T, 100-BASE-T, or similar connection 208 is preferred.

[0037] As described more fully in conjunction with Figure 3, when the network administrator desires to shut down or activate a particular network computer 204, 206, or 208, a shutdown record 210 is generated. Prior to communication over the network, a digital signature of the shutdown record is generated (at element 212). The digital signature is created by first performing a one-way hash function on the shutdown record, followed by encrypting the resulting value with the network administrator's private key. The digital signature is then appended to the shutdown record prior to broadcasting over the network via network interface controller 214.

[0038] The encryption algorithms utilized in element 212 can take many forms, including all of the aforementioned algorithms. The encryption processes are preferably carried out in secure memory that is not readable or writeable and cannot be "sniffed" by surreptitious programs or viruses having the ability to monitor and intercept processes running in normal memory. Such a memory configuration is disclosed, for example, in "METHOD FOR SECURELY CREATING, STORING AND USING ENCRYPTION KEYS IN A COMPUTER SYSTEM," previously incorporated by reference. It is also contemplated that the shutdown record itself could be similarly encrypted prior to broadcast over the network 200.

[0039] The network administrator computer 202 preferably includes network management software such as Compaq Insight Manager. Such software solutions allow an administrator to control and interrogate multiple network computers S and download software (e.g., updated ROM code) to network computers S while they are fully powered. The network management software may incorporate server- or client-based management data collection "agents" and allow network administrators to remotely track and update network node configurations throughout a network 200.

REMOTE CONTROL CAPABILITIES

[0040] In a system implemented according to the Magic Packet™ specification, a method is provided whereby a network administrator or network management software can remotely activate a sleeping network computer S. On the receiving side of the network 200, this is accomplished by enabling power to the network interface controller 122 of a particular network computer S even while the network computer S is in a low power state. The network interface controller 122 monitors the network 200 for a specific Ethernet frame. Each machine on the network is identified by a unique address. In the special Ethernet frame, the targeted network computer's S unique address is repeated sixteen times in a row anywhere within the data field of a valid network frame, serving as a wake-up call. This special frame is referred to as a Magic Packet™ frame.

[0041] As noted, the computer system S also includes power management hardware/software 180 that functions to apply power to the network interface controller 122 when Magic Packet™ mode is enabled. This process can be accomplished through BIOS or other software that is generally aware of the state of the system and capable of setting a bit in the network interface controller 122 to enable Magic Packet™ mode. Alternatively, a network operating system driver configured to monitor Advanced Power Management (APM) calls could be utilized to enable and disable Magic Packet™ mode.

[0042] Through the specialized hardware/software, the network interface controller 122 is also capable of signalling the power management hardware/software 180 to enable power to the network computer S following receipt of a valid Magic Packet™ frame. This signal can be considered analogous to a wake-up event such as a keyboard keystroke or mouse movement. In a contemplated embodiment of the invention, ROM POST code functions to boot the computer system S and return the network interface controller to a normal operating mode following receipt of a wake-up event.

[0043] A Magic Packet™ frame for use with the disclosed embodiment includes sixteen duplications of the address of a particular network computer. S, with no breaks or interruptions. The address sequence can be located anywhere within the Magic Packet™ frame, but is proceeded by a synchronization stream that simplifies the scanning state machine of the network interface controller 122. The synchronization frame is defined as six bytes of "FFh". Preferably, the network interface controller 122 also accepts routed or MULTICAST frames including the sixteen duplications of the address matching the address of the targeted network computer S.

[0044] As an example, assume the address for a particular node on the network is 44h 55h 66h 77h 88h 99h. In this situation, the network interface controller 122 of that node scans for the following data sequence in an Ethernet frame:

[0045] DESTINATION SOURCE MISC FF FF FF FF FF FF 44 55 66 77 88 99 44 55 66 77 88 99 44 55 66 77 88 99 44 55 66 77 88 99 44 55 66 77 88 99 44 55 66 77 88 99 44 55 66 77 88 99 44 55 66 77 88 99 44 55 66 77 88 99 44 55 66 77 88 99 44 55 66 77 88 99 44 55 66 77 88 99 44 55 66 77 88 99 44 55 66 77 88 99 MISC CRC.

[0046] Referring now to Figure 3 a flowchart diagram illustrating generation of a secure network broadcast message in accordance with the present invention is shown. Following commencement of the procedure in step 300, control proceeds to step 302 where the network administrator or network management software

creates a shutdown record for one or more network computers S. When implemented using the Magic Packet™ technology, the shutdown message includes the aforementioned specific data sequence addressing the desired network computers S and indicates to the network interface controllers 122 of these nodes that a Magic Packet™ frame is being broadcast. The shutdown record also includes a control code directing the desired network nodes to enter a low power state. Also included is a secure index (e.g., a time stamp indicating the date and time on which the shutdown record is created).

[0047]   Control next proceeds to step 304 and a secure one-way hash function is performed on the shutdown record, resulting in a hash code representation of the record. In practice, public key algorithms, although capable, are often inefficient when used to sign long documents. In the preferred embodiment of the invention, this problem is addressed by generating a one-way hash of the shutdown record prior to encryption with the network administrator's public key. The hash value is commonly limited to a predetermined length.

[0048]   Preferably, the one-way hash function is performed in a secure manner resistant to snooping or attack by malicious code. Contemplated methods for accomplishing the secure one-way hash function include those illustrated in the previously incorporated references entitled: "SECURE TWO-PIECE USER AUTHENTICATION IN A COMPUTER NETWORK" and "METHOD FOR SECURELY CREATING, STORING AND USING ENCRYPTION KEYS IN A COMPUTER SYSTEM".

[0049]   Following completion of step 304, control next proceeds to step 306 and the secure hash code representation of the shutdown record is encrypted utilizing the network administrator's private key. Again, the encryption process is preferably performed in a secure manner. In essence, step 306 produces a digital signature of the shutdown record that is then appended to the original shutdown record in step 308. Control proceeds to step 310 and the encrypted hash of the shutdown record, in addition to the original shutdown record, is broadcast to a computer network such as that depicted in Figure 2. Control then proceeds to optional step 312 and the network computers' S responses to the broadcast message are recorded.

[0050]   Referring now to Figure 4, a flow chart diagram is provided illustrating the receipt and validation of the secure network broadcast message in accordance with the preferred embodiment of the present invention. This procedure is typically used to verify that the broadcast message was neither modified in transit nor originated from an unauthorized source. Following commencement of the procedure in step 400, control proceeds to step 402 where the network interface controller 122 of the network computer S detects and scans all broadcast messages (or incoming frames).

[0051]   Following detection of a broadcast message, control proceeds to step 404 where the network inter-

face controller 122 examines the broadcast message for a specific data sequence, indicating that the message contains a Magic Packet™ frame. The broadcast message is also examined to determine if it is addressed to the receiving network computer S. If not, control loops to step 406 and the network interface controller 122 awaits the next broadcast message.

[0052]   If the receiving network computer S determines that the broadcast message is directed to it as determined in step 404, control proceeds to step 408 where the digital signature or encrypted hash portion of the received message is decrypted using the administrator's public key. Control next proceeds to step 410 where the network interface controller 122 or other system component performs a one-way hash function on the shutdown record portion of the received message. The decrypted hash of step 408 and the hash function result of step 410 are then compared in step 412. If the two hash values do not match, the broadcast message fails the verification process and control is returned to step 406 to await the next broadcast message. If the broadcast message is validated as secure in step 412, control proceeds to step 414 and the receiving network computer S broadcasts an optional acknowledgement message. Control proceeds to step 416 and the shutdown control code of the broadcast message is executed by the receiving network computer S, which either enters a low power state, awakens, or performs some other predetermined function. The verification process is ended step in 418.

[0053]   For machines in which it is desirable to disable remote control functionality, it is contemplated that the public key of the network administrator can be invalidated such that the specified machine is incapable of detecting a valid broadcast message. This may be desirable for use with network components containing critical or highly sensitive information.

[0054]   Thus, a method has been described for providing secure remote control commands in a distributing computer environment. In the preferred embodiment of the invention, the network administrator or network management software creates a shutdown record, including an index or time stamp, for powering down a specified network computer(s). Prior to broadcast over the network, a secure one-way hash function is performed on the shutdown record. The result of the one-way hash function is encrypted using the network administrator's private key, thereby generating a digital signature that can be verified by specially configured network nodes. The digital signature is appended to the original shutdown record prior to broadcast to the network. Upon receiving the broadcast message, the targeted network computer validates the broadcast message by verifying the digital signature of the packet or frame. The shutdown record or other command code is only executed following authentication of the broadcast message.

7

Claims

1. A method for securely broadcasting remote control commands in a computer network including at least one targeted network computer capable of responding to remote control commands from a network administrator computer or other network computer, the method comprising the steps of:

   generating a remote control command;
   creating a digital signature of the remote control command;
   appending the digital signature to the remote control command to create a broadcast message; and
   communicating the broadcast message to at least one targeted network computer.

2. The method of claim 1, wherein the step of creating a digital signature of the remote control command comprises:

   performing a one-way hash function on the remote control command to generate a signature hash value; and
   encrypting the signature hash value with a private key.

3. The method of claim 2, wherein the targeted network computer(s) further performs the steps of:

   decrypting the signature hash value portion of the broadcast message using a public key corresponding to the private key;
   performing a one-way hash function on the remote control command portion of the broadcast message to generate a verification hash value; and
   comparing the decrypted signature hash value with the verification hash value.

4. The method of claim 3, wherein the targeted network computer(s) further performs the step of:
   executing the remote control command only if the signature hash value and the verification hash value are identical.

5. The method of claim 3, further comprising the step of invalidating the public key corresponding to the private key in at least one network computer such that predetermined remote control commands cannot be validated.

6. The method of any of claims 1 to 5, wherein the targeted network computer(s) further performs the steps of:

   utilizing the digital signature to verify that the broadcast message is authorized; and
   executing the remote control command only if the broadcast message is authentic and authorized.

7. The method of any of claims 1 to 6, wherein the remote control command includes an index or time stamp.

8. The method of any of claims 1 to 6, wherein the remote control command directs the targeted network computer to enter a low power state.

9. The method of any of claims 1 to 6, wherein the remote control command directs the targeted network computer to enter a fully powered state.

10. The method of claim 2 on any claim when dependent thereon, wherein the private key is maintained in secure memory space.

11. The method of any of claims 1 to 10, wherein the step of communicating the broadcast message to at least one targeted network computer is substantially compliant with the Magic Packet™ specification.

12. The method of any of claims 1 to 11, wherein the digital signature is generated during a secure mode of operation or in secure computer memory.

13. A computer system configured to receive secure network communications, the secure network communications having a remote control command and a digital signature, the computer system comprising:

   a system bus;
   a processor coupled to the system bus;
   power management hardware or software; and
   network interface circuitry coupled to the system bus and the power management hardware or software, the network interface circuitry configured to perform or direct the steps of:

   utilizing the digital signature to verify that the broadcast message is authentic; and
   permitting the execution of the remote control command only if the broadcast message is authentic, wherein the remote control command causes a change in state in the power management hardware or software.

14. A computer system according to claim 13, further comprising:
   a mass storage device coupled to the system bus.

15. The computer system of claim 13 or claim 14, wherein the change in state in the power management hardware or software causes the computer system to enter a low power mode.

16. The computer system of claim 13 or claim 14, wherein the change in state in the power management hardware or software causes the computer system to become fully powered.

17. The computer system of any of claims 13 to 16, wherein the digital signature comprises a hash code representation of the remote control command, the hash code representation encrypted with a private key, and wherein the step of utilizing the digital signature to verify that the broadcast message is authentic comprises:

decrypting the signature hash code representation of the broadcast message using a public key corresponding to the private key;
performing a one-way hash function on the remote control command portion of the broadcast message to generate a verification hash value; and
comparing the decrypted hash code representation of the broadcast message with the verification hash value.

18. The computer system of any of claims 13 to 17, wherein the network interface circuitry is further configured to substantially comply with the Magic Packet™ specification.

19. The computer system of any of claims 13 to 18, further comprising a non-writeable secure memory space coupled to the processor, wherein the public key is maintained in the secure memory space.

20. A computer system configured to broadcast secure computer network communications, the computer system comprising:

a system bus;
a processor coupled to the system bus;
a processor readable storage medium coupled to the system bus for directing the processor to perform the steps of:

generating a remote control command;
creating a digital signature of the remote control command; and
appending the digital signature to the remote control command to create a broadcast message;

network interface circuitry coupled to the system bus, the network interface circuitry respon-

sive to a command(s) from the processor to transmit the broadcast message to a computer network.

21. A computer system according to claim 20, further comprising:

a mass storage device coupled to the system bus.

22. The computer system of claim 20 or claim 21, wherein the step of creating a digital signature of the remote control command comprises the steps of:

performing a one-way hash function on the remote control command to generate a signature hash value; and
encrypting the signature hash value with a private key.

23. The computer system of any of claims 20 to 22, wherein the broadcast message is substantially compliant with the Magic Packet™ specification.

24. The computer system of any of claims 20 to 23, wherein the remote control command includes an index or time stamp.

25. The computer system of any of claims 20 to 23, further comprising a secure memory space coupled to the processor, wherein the private key is maintained in the secure memory space.

FIG. 1

FIG. 2

NETWORK COMPUTERS S
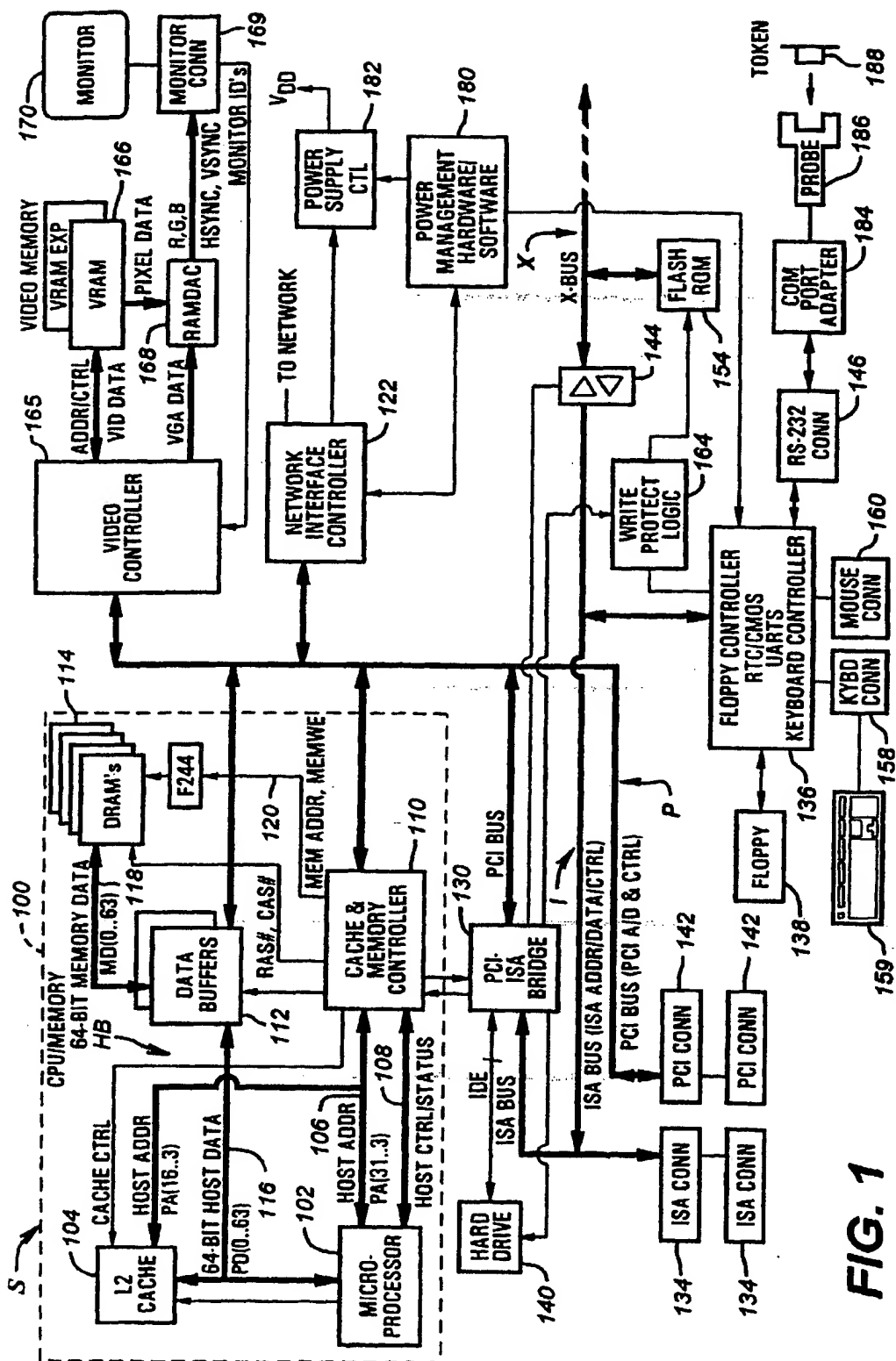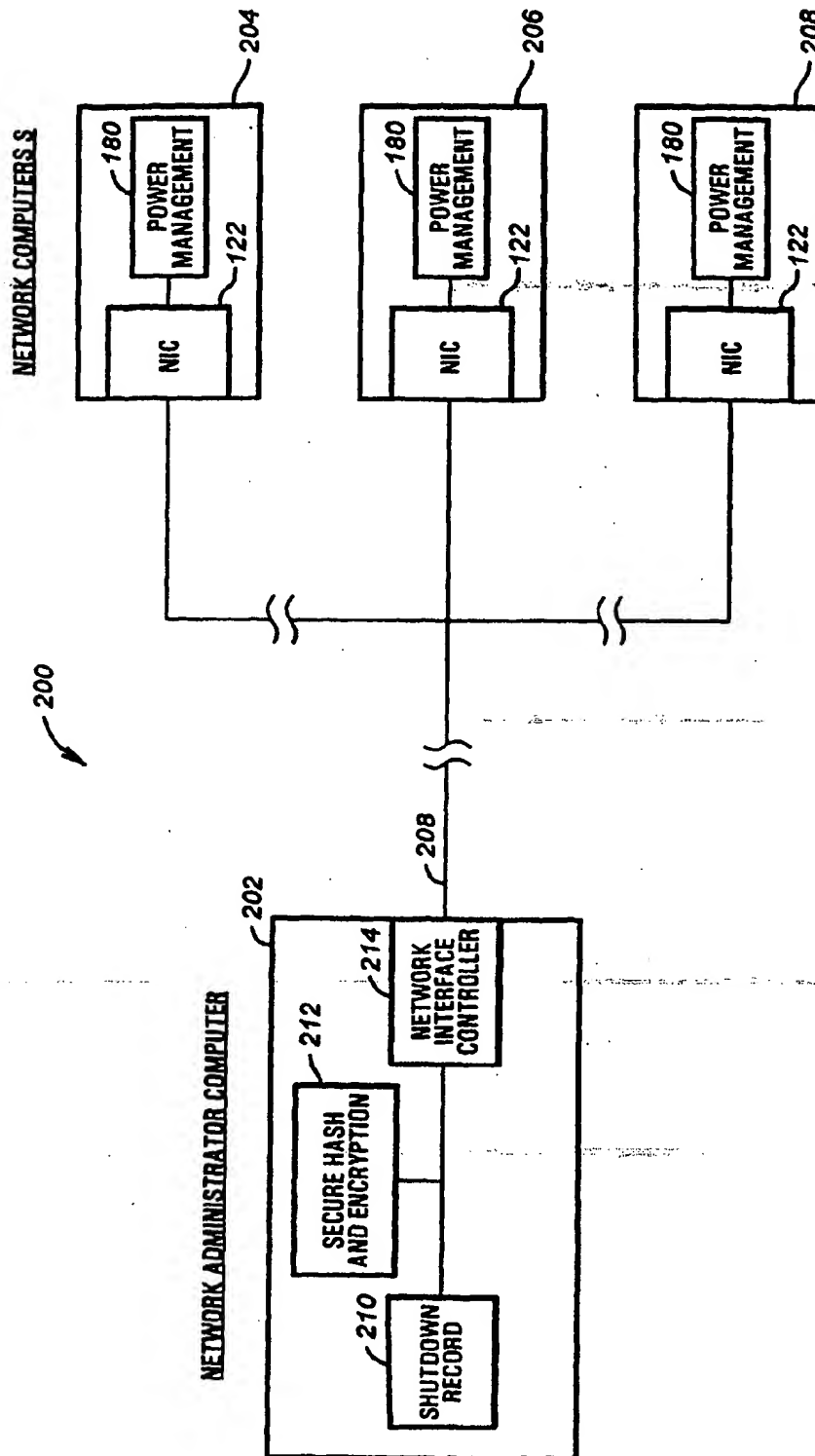
204
180
POWER MANAGEMENT
NIC
122

206
180
POWER MANAGEMENT
NIC
122

208
180
POWER MANAGEMENT
NIC
122

200

208

NETWORK ADMINISTRATOR COMPUTER

202

212
SECURE HASH AND ENCRYPTION

214
NETWORK INTERFACE CONTROLLER

210
SHUTDOWN RECORD

11

START — 300

CREATE SHUTDOWN
RECORD (INCLUDING
TIMESTAMP) — 302

GENERATE
SECURE HASH
OF RECORD — 304

ENCRYPT HASH WITH
ADMINISTRATOR'S
PRIVATE KEY — 306

APPEND ENCRYPTED
HASH TO SHUTDOWN
RECORD — 308

BROADCAST ENCRYPTED
HASH + SHUTDOWN
RECORD TO NETWORK — 310

RECORD RESPONSES
TO BROADCAST
(OPTIONAL) — 312

END
PROCEDURE — 314

FIG. 3

START — 400

DETECT BROADCAST MESSAGE — 402

PACKET FOR THIS NODE ? — 404

N → AWAIT NEXT BROADCAST MESSAGE — 406

Y

DECRYPT HASH PORTION OF RECEIVED MESSAGE USING ADMINISTRATOR'S PUBLIC KEY — 408

GENERATE HASH OF SHUTDOWN RECORD PORTION OF RECEIVED MESSAGE — 410

HASHES MATCH ? — 412

N →

Y

ACKNOWLEDGE BROADCAST MESSAGE (OPTIONAL) — 414

EXECUTE CONTROL CODE (SHUTDOWN) — 416

END — 418

FIG. 4